Listing of All Claims Including Current Amendments

1.   (currently amended) A document security system for printing secured documents comprising:

a digital file accessible by a receiver via a terminal;

a printer connected to the terminal;

security data specific to each page of said digital file; and

a printed file printed by said printer corresponding to said digital file;

a mark printed by said printer on each page of the printed ~~digital~~ file, said mark containing data unique to each page of the printed ~~digital~~ file;

wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented by means of the mark containing data unique to each page of the printed file.

2.   (original) The document security system for printing secured documents according to claim 1 wherein said printer is connected to said terminal via a network connection.

3.   (original) The document security system for printing secured documents according to claim 1 further comprising an identification device for identifying the sender.

4.   (original) The document security system for printing secured documents according to claim 3 wherein a second identification device is provided at the printer wherein the printer will not print said digital document unless identification data gathered by the second identification device matches stored identification data of users that are allowed access to said digital document.

5.   (original) The document security system for printing secured documents according to claim 3 wherein said identification device comprises a fingerprint keypad.

6.   (original) The document security system for printing secured documents according to claim 1 wherein the security system encrypts said digital file prior to said digital file being sent to the printer.

7.   (original) The document security system for printing secured documents according to claim 1 wherein said mark is selected from the group consisting of: a Watermark or an Optical Variable Device.

8.   (original) The document security system for printing secured documents according to claim 1 wherein said mark comprises DNA information coded in ink utilized to print said mark.

9.   (original) The document security system for printing secured documents according to claim 1 wherein the characteristics of said mark are selected from the group consisting of covert data, overt data or combinations thereof.

10.   (original) The document security system for printing secured documents according to claim 1 wherein said mark is printed on a medium, said medium selected from the group consisting of: plain paper, paper having a distinct pattern located thereon, or thermal transfer holographic foil.

11.   (original) The document security system for printing secured documents according to claim 1 wherein said printer uses ink to print said digital file, said ink selected from the group consisting of: DNA ink or fluorescent ink.

12.   (original) The document security system for printing secured documents according to claim 1 further comprising verification data gathered by the security system for verifying whether the sender has clearance access said digital file.

13.   (original) The document security system for printing secured documents according to claim 10 wherein said verification data includes identification of the sender.

14.   (original) The document security system for printing secured documents according to claim 10 wherein the security system selectively grants the user access to said digital file based upon the collected verification data.

15.   (currently amended) A document security system for printing secured documents comprising:

a digital file accessible by a sender via a terminal, said digital file comprising at least two pages to be printed;

a printer connected to the terminal via a network;

a printed file printed by said printer corresponding to said digital file;

security data specific to each page of the printed ~~digital~~ file; and

at least two marks printed by said printer on the at least two pages of the printed ~~digital~~ file, said marks containing data unique to each of the at least two pages of the printed ~~digital~~ file;

wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented by means of the mark containing data unique to each page of the printed file.

16.   (original) The document security system for printing secured documents according to claim 15 further comprising verification data gathered by the security system for verifying whether the sender has clearance access said digital file.

17.   (original) The document security system for printing secured documents according to claim 16 wherein said verification data includes identification of the sender.

18.   (original) The document security system for printing secured documents according to claim 15 wherein the security system encrypts said digital file prior to said digital file being sent to said printer.

19.   (original) The document security system for printing secured documents according to claim 15 wherein said mark is a watermark.

20.   (original) The document security system for printing secured documents according to claim 15 wherein the characteristics of said mark are selected from the group consisting of covert data, overt data or combinations thereof.

21.   (currently amended) A method for printing secured documents comprising the steps of:

        collecting verification data from a sender relating to a digital file;

        verifying access to the digital file based upon the collected verification data;

        accessing the digital file;

        inputting a print command;

        generating security data related to the verification data, the security data being specific to each page of the digital file to be printed;

        encrypting the digital file;

        sending the encrypted digital file to a printer; and

        printing the digital file with a mark on each page of the document, the mark for each page containing data unique to each page of the printed document;

        wherein unauthorized copying and/or alteration of the printed document is prevented <u>by means of the mark containing data unique to each page of the printed document</u>.

22.   (original) The method for printing secured documents according to claim 21 further comprising the steps of selectively granting the sender access to the digital file based upon the collected verification data.

23.   (original) The method for printing secured documents according to claim 21 wherein the verification data includes identification of the sender.

24.   (original) The method for printing secured documents according to claim 21 wherein the mark comprises a watermark.

25.   (original) The method for printing secured documents according to claim 21 wherein the characteristics of the mark are selected from the group consisting of covert data, overt data or combinations thereof.

26.   (currently amended) A method for printing secured documents comprising the steps of:
        accessing the digital file;
        generating security data related to the digital file, the security data being specific to each page of the digital file to be printed;
        sending the digital file to a printer;
        printing the digital file and a mark on each page of the digital file, the mark containing data unique to each page of the printed ~~digital~~ file;
        wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented <u>by means of the mark containing data unique to each page of the printed file</u>.

27.   (currently amended) A document security system for printing secured documents comprising:
        a digital file accessible by a receiver via a computer terminal;
        security data specific to said digital file and to each page of said digital file;

a printer connected to the computer terminal; and

a mark printed by said printer on each page of the printed ~~digital~~ file, said mark containing data unique to each page of the printed ~~digital~~ file;

wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented <u>by means of the mark containing data unique to each page of the printed file</u>.

28.   (currently amended) A document security system for printing secured documents comprising:

a digital file accessible by a receiver via a computer;

a printer connected to the computer;

security data specific to said digital file;

ink usable by said printer, said ink having coded DNA information that contains said security data specific to said digital file; and

a mark printed by said printer with said ink on the printed ~~digital~~ file, said mark containing data specific the printed ~~digital~~ file;

wherein said security data further comprises data unique to each page of said ~~digital~~ file and said mark further contains data unique to each page of said ~~digital~~ file; and

wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented <u>by means of the mark containing data unique to each page of the printed file</u>.

29.   (cancelled)

30.   (currently amended) A document security system for printing secured documents comprising:

a digital file accessible by a receiver via a computer;

a printer connected to the computer;

security data specific to said digital file; and

an Optical Variable Device printed by said printer on each page of the printed ~~digital~~ file, said Optical Variable Device containing data specific the printed ~~digital~~ file;

wherein said security data further comprises data unique to each page of said digital file and said Optical Variable Device further contains data unique to each page of said digital file; and

wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented <u>by means of the mark containing data unique to each page of the printed file</u>.

31.   (cancelled)

32.   (currently amended) A document security system for printing secured documents comprising:

a digital file accessible by a sender via a terminal;

a printer connected to the terminal via a network connection;

security data specific to each page of said digital file; and

a mark printed by said printer on each page of the printed ~~digital~~ file, said mark containing data unique to each page of the printed ~~digital~~ file;

wherein unauthorized copying and/or alteration of the printed ~~digital~~ file is prevented <u>by means of the mark containing data unique to each page of the printed file</u>.